Clinia Santé inc.
3572 Dorion
Montréal, (Québec), H2K 4B6

ANALYSE DE RISQUES LIÉS À L'UTILISATION DE DONNÉES SENSIBLES

Préparé pour:

Clinia Santé Inc.

Préparé par:

Guillaume Poirier, *Conseiller en politiques de sécurité*

Table des matières

1. Mise en contexte

Afin d'informer les utilisateurs du système d'information sur les enjeux relié à l'utilisation des données sensibles des professionnels de la santé, l'entreprise à décider de conduire une analyse de risque et de la rendre publique. Cette analyse de risque suit la méthodologie **PRIAM** [1] (*Privacy Risk Analysis Methodology*) qui consiste en deux phases principales. La première est la collecte d'information et la deuxième est l'évaluation des risques. L'objectif final de cet exercice est de définir les sources de risques potentiels, les vulnérabilités possibles du système, les conséquences de l'exploitation desdites vulnérabilités ainsi que les préjudices potentiels qui pourraient être causés aux individus concernés par les données sensibles.

1.1. Données sensibles

Le système d'information manipule plusieurs types de données et ce ne sont pas tous les types de données qui sont visés par cette analyse de risque. Pour la suite, on qualifiera les données visées par cette analyse comme étant de "données sensibles". Ce qu'on qualifie de donnée sensible, ce sont les données qui concernent les professionnels de la santé. Les données sensibles ne sont pas, par définition, des données personnelles et possèdent donc un caractère moins confidentiel que des données personnelles. Quand on parle de données personnelles, on parle de données financières, des données qui décrivent les habitudes de vies du sujet ou encore des données les numéros d'assurance sociale et les numéros de permis de conduire. Le système dans son ensemble manipule les données sensibles suivantes en lien avec les professionnels de la santé :

- Prénom;
- Nom;
- Numéro de permis;
- Titre (p. ex. M., Mme, Dr, Dre, etc.);
- Sexe;
- Informations de contact (téléphones, fax, courriels, sites web et pagettes);
- Spécialités (p. ex. dermatologie, cardiologie, podiatrie, etc.);
- Lieux de travail;
- Plages horaires;
- Réseaux sociaux;

[1] Pour plus d'information sur la méthodologie **PRIAM**, consulter https://hal.inria.fr/hal-01302541/document

Les attributs de ces données sont :

- *Sensibilité* :

  Toutes les données sauf les informations de contact sont d'ordre public et ne sont donc pas sensibles. Les informations de contact sont considérées comme sensibles, sauf quand elles sont obtenues via des registres et répertoires publics.

- *Forme* :

  Encrypté durant la transmission et décrypté durant la manipulation et l'affichage. Tous les systèmes et les acteurs doivent s'authentifier avant de consulter les données.

- *Origine* :

  Les données sont obtenues via des registres et répertoires publics ou peuvent être saisies par les utilisateurs du système.

- *Utilisation* :

  Les données sont utilisées par les utilisateurs afin de faciliter l'accès aux ressources de la santé ainsi qu'au transfert d'information pertinente entre les différents acteurs de l'écosystème de la santé.

- *Rétention* :

  Les données sont conservées tant et aussi longtemps qu'un utilisateur ne la supprime pas. La donnée peut potentiellement exister dans plusieurs espaces de travail de plusieurs partenaires et sa durée de vie à l'intérieur de chacun de ces espaces de travail est indépendante des autres.

- *Visibilité* :

  Les données sont visibles aux utilisateurs du **CMS** et du **SearchAPI**, ainsi qu'au personnel autorisé à effectuer des opérations de soutien et de maintenance sur le système.

- *Intervention* :

  Aucune. Le professionnel de la santé n'a aucun pouvoir d'intervention sur les données le concernant. Seuls les utilisateurs peuvent modifier ou supprimer une donnée.

2. Définition du système

L'analyse de risque débute avec la définition du système qui lui-même permet la définition des frontières logiques de l'analyse de risque. La définition du système doit englober le cycle de vie

complet des données sensibles à l'intérieur des applications. On peut donc affirmer qu'il est composé de plusieurs composants matériels et logiciels.

2.1. Spécifications fonctionnelles

L'outil de répertoire et de recherche est composé des sous-systèmes suivants :

- Un **SearchAPI** qui permet aux utilisateurs d'effectuer des recherches et de consulter des données;
- Un **Content Management System** (**CMS**) qui permet aux utilisateurs de consulter et de modifier les données;
- Un **CMS User interface** (**CMSUI**) qui permet aux utilisateurs d'interagir avec le **CMS**;
- Un **User Management System** (**UMS**) qui permet aux administrateurs de gérer les comptes des utilisateurs ainsi que les permissions qui leur sont associés;
- Un **UMS User interface** (**UMSUI**) qui permet aux administrateurs d'interagir avec le **UMS**;
- Un Authentication System (**AS**) qui permet aux utilisateurs et aux administrateurs de s'authentifier afin d'interagir avec les autres sous-systèmes;
- Un système automatisé de mise à jour des données (**ETL**) qui met à jour des données dans les espaces de travail des clients;
- Un **User Data Store** (**UDS**) qui sert de base de données utilisateur;
- Un **Health Resource Data Store** (**HRDS**) qui sert de base de données pour les données sur les ressources de la santé;
- Un **Search Data Store** (**SDS**) qui sert de base de données pour les données sur les ressources de la santé et qui est optimisé pour la recherche;

2.2. Flux de données

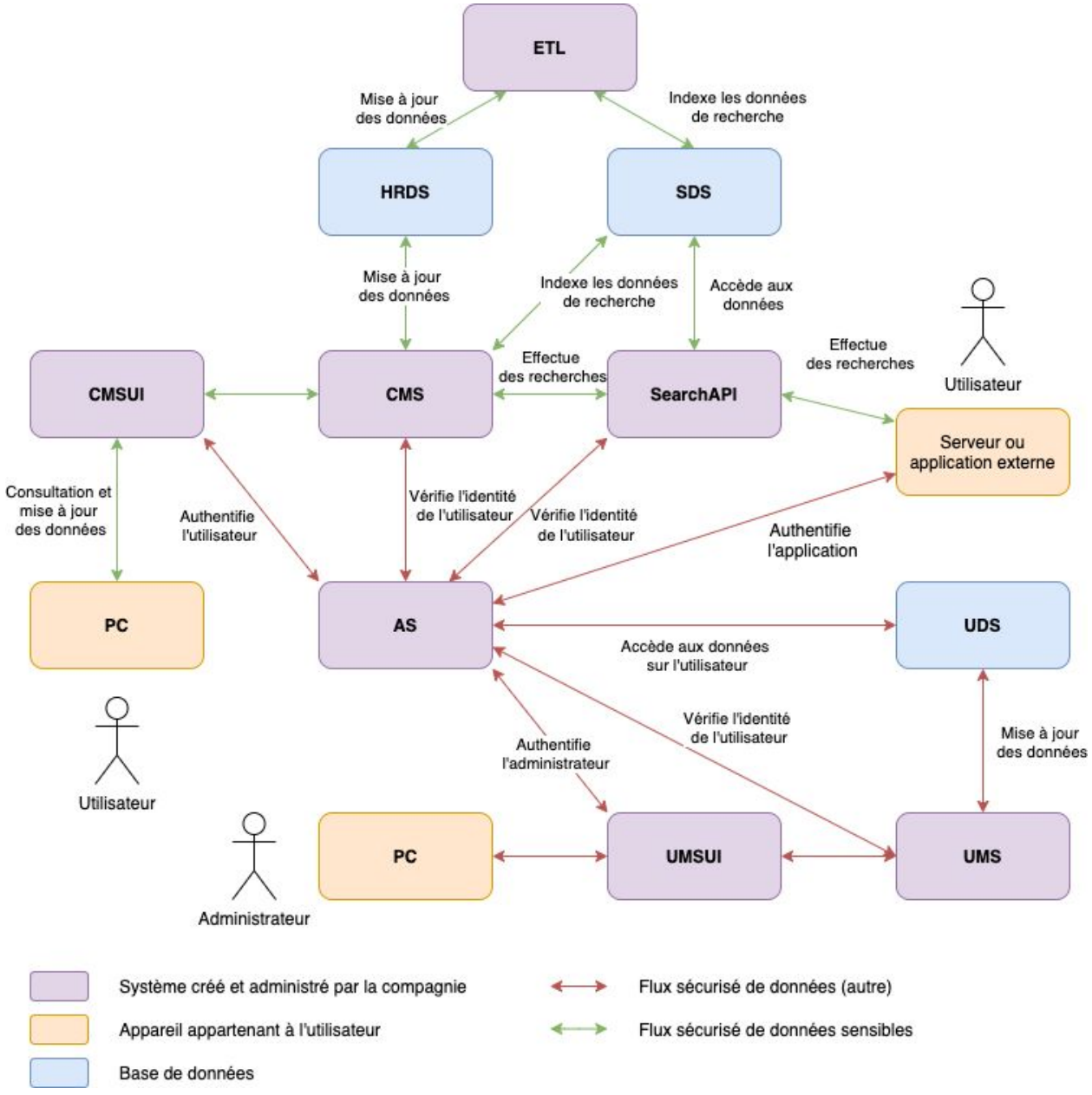

Figure 1 : Flux de données dans le système d'information

2.3. Acteurs

Les acteurs suivants interagissent avec l'outil de répertoire et de recherche :

- Utilisateurs;
- Administrateurs;
- Développeurs;
- Autres employés de l'entreprise;

2.4. Mesures de contrôles

Techniques

- Authentification requise pour tous les utilisateurs avant d'accéder aux données sensibles, peu importe par quel système ou sous-système l'accès est fait;
- Les mots de passe des utilisateurs sont toujours encryptés;
- Politique de sécurité des mots de passe mis en place afin d'assurer la robustesse des mots de passe choisis par les utilisateurs;
- Toutes les transactions sont journalisées dans un serveur de journalisation distant;
- Les journaux sont revus de façon périodique afin d'identifier des actions suspectes;
- Détection d'évènements inhabituels dans le système afin d'alerter les administrateurs;
- Protection des journaux afin de limiter l'accès aux personnes non autorisées;
- Limite d'impressions des données sensibles dans les journaux;
- Désactivation d'un compte utilisateur après une certaine période d'inactivité;
- Verrouillage d'un compte utilisateur après un trop grand nombre de tentatives de connexion erronées;
- Un administrateur peut désactiver le compte d'un utilisateur de son espace de travail en tout temps;
- Un individu ne peut pas se créer de compte sans avoir été invité par un administrateur d'un espace de travail;
- L'accès aux données est protégé à l'aide de contrôle d'accès;
- Limite du nombre de résultats de recherche retourné via le **SearchAPI**;
- Le **CMSUI** ne permet pas la sauvegarde locale d'information sur un poste de travail;
- Utilisation de jeton et de témoins afin d'identifier et d'authentifier les utilisateurs qui communique avec les CMS, le **SearchAPI** et le UMS;
- Les communications entre le **CMS** et le **CMSUI** sont encryptées à l'aide de TLS;
- Les communications entre le **UMS** et le **UMSUI** sont encryptées à l'aide de TLS;
- Les communications entre le **SearchAPI** et les applications externes sont encryptées à l'aide de TLS;

Organisationnelles

- Présence d'une forte politique de sécurité des actifs informationnels;
- Formation régulière des employés sur la sécurité;
- Assignation de droits d'accès restreints à tous les employés de l'entreprise;
- Présence d'un plan de reprise des activités en cas de sinistre;
- Présence d'un plan de réponse aux incidents de sécurité;
- Présence de plusieurs procédures en lien avec l'application des politiques de sécurité ainsi que des demandes de changements aux politiques de sécurité;

Légales

- Présence d'une clause sur la confidentialité de l'information dans les contrats avec les partenaires;
- Présence d'une clause sur la confidentialité de l'information dans les contrats avec les employés;
- Présence d'une clause de confidentialité et des termes de services de l'outil CMS lors de la création d'un nouveau compte. L'utilisateur doit accepter les termes de services avant d'avoir accès aux données;

2.5. Source de risques

Une source de risque est une entité (individu ou organisation) qui peut accéder (légalement ou illégalement) aux données sensibles et dont les actions peuvent directement ou indirectement, intentionnellement ou non intentionnellement mener à des dommages en lien avec la confidentialité de l'information.

Une fois les sources de risques ainsi que leurs attributs sont identifiés (Tableau 1), on définit, pour chacune, sa capacité à exploiter des vulnérabilités. L'échelle de cette capacité est la suivante :

- *Élevé* si la majorité des attributs favorisent une exploitation;
- *Moyen* si la quelques attributs favorisent une exploitation;
- *Bas* si peu des attributs favorisent une exploitation;

Code	Categorie	Individu/Organisation	Interne/Externe	Valeur de l'exploit	Motivation/Peur de répercussions	Information	Droits d'accès aux données sensibles	Outils/Connaissances	Relation avec le sujet
A1	Fournisseur de service (Clinia)	Organisation	Interne	Élevé	Élevé	Connaissance accrue du système	Toutes les données	Élevé	Semi confiance
A2	Administrateur compromis	Individu	Interne	Élevé	Moyen	Connaissance accrue du système	Aucune	Moyen	Aucune
A3	Utilisateur compromis	Individu	Interne	Élevé	Moyen	Bonne connaissance du système	Les données de son espace de travail	Moyen	Aucune
A4	Pirate informatique	Individu/Organisation	Externe	Élevé	Élevé	-	Aucune	Élevé	Aucune
A5	Développeur compromis	Individu	Interne	Élevé	Moyen	Connaissance accrue du système	Aucune	Élevé	Aucune
A6	Personnel de soutien compromis	Individu	Interne	Élevé	Moyen	Connaissance accrue du système	Aucune	Moyen	Aucune

Tableau 1 : Sources de risques et leurs attributs

2.6. Vulnérabilités

Une vulnérabilité est définie comme étant une faiblesse dans les mécanismes de protection des données (elle peut être technique, organisationnelle ou légale) du système ou encore d'une absence de mécanisme qui peut ultimement résulter en un bris de confidentialité.

Les vulnérabilités incluent :

- Les vulnérabilités introduites de façon intentionnelle lors de la conception ou le design du système;
- Les erreurs dans la conception ou le design du système;
- Les erreurs d'implémentation dans la réalisation du système;

À ces vulnérabilités (Tableau 2), on assigne une facilité d'exploitation qui suit l'échelle suivante :

- *Élevé* si la vulnérabilité est facile à exploiter ou si les données accessibles sont elles-mêmes faciles à exploiter;
- *Moyen* si la vulnérabilité est modérément difficile à exploiter ou si les données accessibles sont elles-mêmes modérément difficiles à exploiter;
- *Bas* si la vulnérabilité est difficile à exploiter ou si les données accessibles sont elles-mêmes difficiles à exploiter;

Code	Vulnérabilité	Exploitabilité
V1	Transmission non sécurisée de données	Moyen
V2	Audit du système insuffisant	Élevé
V3	Contournement de la limite de résultats de recherche	Élevé
V4	Accès aux journaux du système	Bas
V5	Erreurs fonctionnelles dans le **SearchAPI**	Bas
V6	Erreurs fonctionnelles dans le **AS**	Bas
V7	Erreurs fonctionnelles dans le **CMS**	Bas
V8	Erreurs fonctionnelles dans le **CMSUI**	
V9	Vulnérabilité de sécurité dans le **SearchAPI**	Élevé
V10	Vulnérabilité de sécurité dans le **AS**	Élevé
V11	Vulnérabilité de sécurité dans le **CMS**	Bas
V12	Vulnérabilité de sécurité dans le **CMSUI**	Moyen
V13	Échec de la politique de mots de passe robustes	Moyen
V14	Échec de la détection d'évènements inhabituels	Bas
V15	Usurpation de jetons et de témoins afin d'obtenir des accès non autorisés	Élevé
V16	Échec de la mise en vigueur des politiques de sécurité lors de l'utilisation du système par les partenaires	Moyen

Tableau 2 : Vulnérabilités et leurs attributs

2.7. Événements redoutés

Un événement redouté est un événement du système qui se produit en conséquence à l'exploitation d'une ou de plusieurs vulnérabilités et qui peut porter atteinte au bien-être d'un individu ou d'un groupe d'individu. Les événements redoutés (Tableau 3) sont définis en lien avec les attributs des données sensibles. À ces événements, on assigne deux attributs principaux qui sont :

- L'*ampleur*, qui décrit le nombre d'individus potentiellement affecté par la réalisation d'un événement redouté;
    - *Élevé* si tous les individus sont affectés;
    - *Moyen* si plusieurs individus sont affectés;
    - *Bas* si un seul individu est affecté;
- L'*irréversibilité*, qui décrit la difficulté avec laquelle peut être renversé un événement redouté;

Code	Événements redoutés	Scénarios pertinents	Ampleur	Irréversibilité
ER1	Sauvegarde de données personnelles sur les ressources de la santé qui ne sont pas définies dans les données sensibles.	Un partenaire ne respecte pas les politiques de sécurité du **CMS** entre des informations personnelles dans des champs qui ne sont pas prévus à cet effet.	Moyen	Moyen
ER2	Utilisation des données à des fins non autorisées.	Envoi de publicité ciblé, envoyé des demandes de rendez-vous abusives	Élevé	Élevé
ER3	Accès non autorisé aux données.	Un criminel obtient les données sensibles	Élevé	Élevé

Tableau 3 : Événements redoutés et leurs attributs

2.8. Préjudices

On définit un préjudice comme une conséquence négative sur un sujet de données sensibles, sur un groupe de sujets de données sensibles ou sur la société dans son ensemble. Les impacts négatifs peuvent être physiques, psychologiques, financiers, porter atteinte à la dignité ou à la réputation du sujet, ou encore brimer les droits et libertés de ceux-ci. Les préjudices sont les conséquences de la concrétisation d'un événement redouté. À ces préjudices, on assigne deux attributs qui sont :

- *Victime*, qui définit le nombre d'individus affecté par le préjudice;
    - *Élevé* si l'ensemble de la société est affectée;
    - *Moyen* si un groupe d'individus est affecté;
    - *Bas* si un seul individu et ses proches sont affectés;
- L'*intensité*, qui définit l'intensité des impacts négatifs que subissent le ou les sujets;
    - *Élevé* si le préjudice provoque une perte d'emploi, la révélation de détails embarrassants sur la vie privée au public, atteinte à la réputation qui résulte en des pertes financières importantes;
    - *Moyen* si le préjudice provoque la révélation de détails embarrassants sur la vie privée aux proches du sujet, atteinte à la réputation ne résultant pas en pertes financières;
    - *Bas* si le préjudice provoque l'envoi de publicité ciblée et l'envoi de courrier ou de contact non sollicité;

Une fois ces deux premiers attributs définis, on peut assigner un dernier attribut au préjudice qui est une composition des deux autres attributs. On peut voir les valeurs de cet attribut dans le *Tableau 4*. On peut ensuite voir les préjudices ainsi que leurs attributs dans le *Tableau 5*.

Sévérité	***Victime***	***Intensité***
Négligeable	Bas	Bas
Limité		Moyen
Significatif		Élevé
Limité	Moyen	Bas
Significatif		Moyen
Maximum		Élevé
Significatif	Élevé	Bas
Maximum		Moyen
Maximum		Élevé

Tableau 4 : Sévérité d'un préjudice en fonction de ses autres attributs

Code	Exemple d'événement	Catégorie	Victime	Intensité	Sévérité
H1	Dévoilement indésirable de données sensibles au public	Psychologique	Moyen	Bas	Limité
H2	Dévoilement indésirable de données personnelles au public	Psychologique, Financière	Moyen	Élevé	Maximum

Tableau 5 : Préjudices et leurs attributs

3. Évaluation des risques

Une fois la phase de collecte d'informations terminée, on peut effectuer la phase d'évaluation des risques. On a établi précédemment qu'un préjudice est la conséquence de la concrétisation d'un ou de plusieurs événements redoutés, qui eux-mêmes sont possibles parce que des vulnérabilités potentielles existent dans le système. Afin de calculer la probabilité qu'un préjudice soit causé à un sujet des données sensibles, on construit des arbres de préjudices. Un arbre de préjudices a comme racine un préjudice et chaque feuille de l'arbre représente une vulnérabilité exploitable par la source de risque le plus plausible. Les embranchements de cet arbre sont des noeuds *ET* et *OU* qui dénotent si les vulnérabilités ou événements redoutés sont tous nécessaires à la concrétisation d'un préjudice, ou si un seul d'entre eux l'est.

À chacune des feuilles, on assigne aussi une probabilité qui est le résultat de la concaténation de l'exploitabilité de la vulnérabilité avec le niveau de risque associé à la source qui l'exploite (*Tableau 6*).

Probabilité d'exploitation	***Exploitabilité***	***Niveau de risque***
Négligeable	Bas	Bas
Limité		Moyen
Intermédiaire		Élevé
Limité	Moyen	Bas
Significatif		Moyen
Maximum		Élevé
Intermédaire	Élevé	Bas
Maximum		Moyen
Maximum		Élevé

Tableau 6 : Probabilité en fonction de l'exploitabilité et du niveau de risque

Une fois l'arbre mis en place et les probabilités assignées aux feuilles, on peut remonter l'arbre en suivant les règles suivantes de façon à obtenir la probabilité finale qu'un préjudice soit causé au sujet des données sensibles :

- Noeud *ET* avec des enfants indépendants : $\Pi_i P_i$
- Noeud *ET* avec des enfants dépendants : $Min_i (P_i)$
- Noeud *OU* avec des enfants indépendants: $1 - \Pi_i (1 - P_i)$
- Noeud *OU* avec des enfants dépendants: $\Sigma_i (P_i)$

On utilise les valeurs symboliques suivantes afin de calculer les probabilités :

- *Négligeable* (N) pour $p < 0.01\%$
- *Limité* (L) pour $0.01\% \leq p < 0.1\%$
- *Intermédiaire* (I) pour $0.1\% \leq p < 1\%$
- *Significatif* (S) pour $1\% \leq p < 10\%$
- *Maximum* (M) pour $p \geq 10\%$

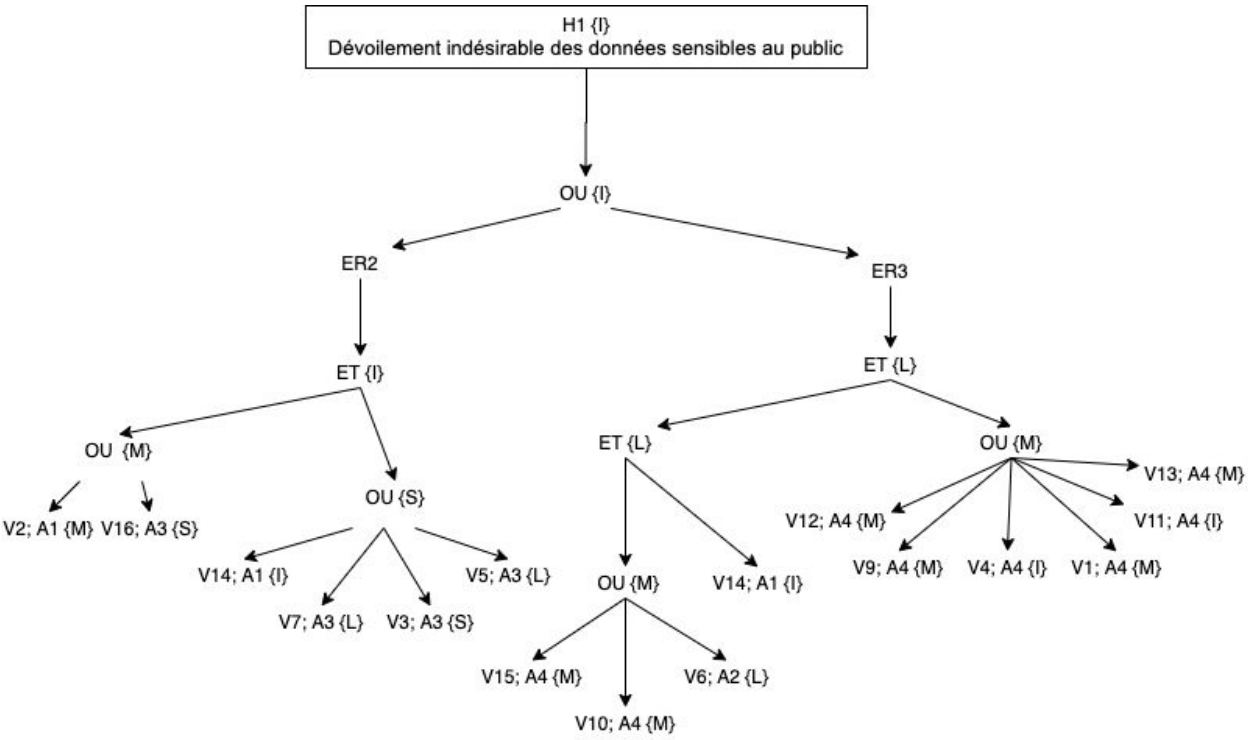

Figure 2 : Arbre de préjudice H1

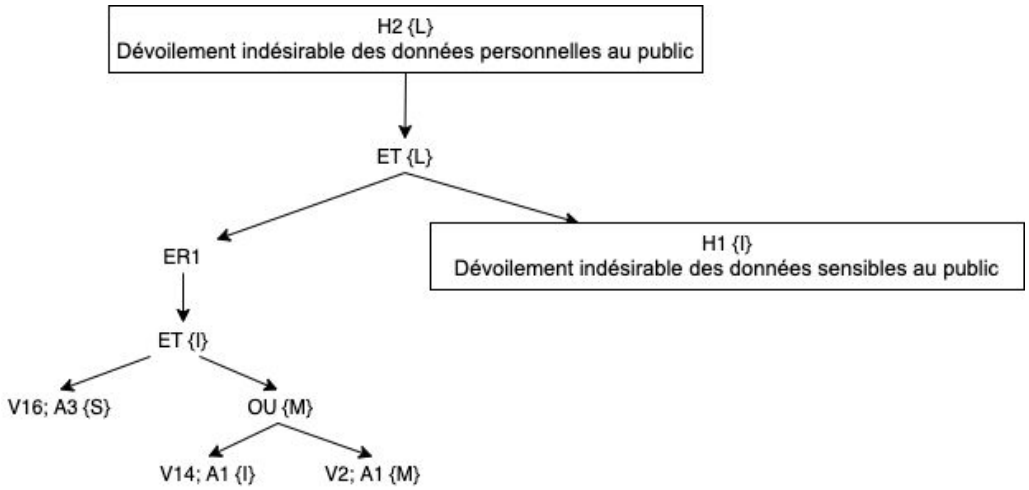

Figure 3 : Arbre de préjudice H2

4. Conclusion

À la lumière de l'analyse, on conclut que la paire {*probabilité*, *sévérité*} pour chacun des préjudices est :

- H1 Dévoilement des données sensibles au public = {*intermédiaire*, *limité*}
- H2 Dévoilement des données personnelles au public = {*limité*, *maximum*}

Puisque la sévérité d'un préjudice est inhérente à la magnitude des dommages causés par celui-ci, elle ne peut être réduite. Le seul facteur sur lequel on peut agir est la probabilité qu'un tel préjudice se réalise, ce qui dépend directement de la probabilité qu'un événement redouté se concrétise.

Clinia travaille d'arrache-pied afin de s'assurer que les données sensibles de ses partenaires préservent leur caractère confidentiel. La mise en ligne publique de cette analyse de risques fait foie de notre transparence ainsi que de notre désir de s'assurer que les données qui sont confiées à l'entreprise soient manipulées de façon sécuritaire. C'est dans cette optique que Clinia a élaboré une forte politique de sécurité des actifs informationnels ainsi qu'un plan de réponse aux incidents de sécurité. On s'assure aussi que les processus et procédures de sécurité soient respectés à l'aide d'audit interne et externe.

La priorité de l'entreprise est, et restera toujours, de faciliter l'accès aux soins de santé pour tous, sans compromis sur la sécurité.

Suivi des changements

***A - Ajouté, M - Modifié, S - Supprimé**

VERSION	DATE	NUMÉRO DE FIGURE, TABLE OU SECTION	AMS*	DESCRIPTION DU CHANGEMENT
1.0	2020-04-16	Tout le document	A	Initialisation document.
1.1	2020-04-20	Tout le document	M	Correction.